UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/814,608	03/30/2004	Antonio Lain	B-5407 621797-2	5425

22879 7590 03/31/2010

HEWLETT-PACKARD COMPANY
Intellectual Property Administration
3404 E. Harmony Road
Mail Stop 35
FORT COLLINS, CO 80528

EXAMINER	
WRIGHT, BRYAN F	

ART UNIT	PAPER NUMBER
2431	

NOTIFICATION DATE	DELIVERY MODE
03/31/2010	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

JERRY.SHORMA@HP.COM
ipa.mail@hp.com
laura.m.clark@hp.com

Office Action Summary	Application No.	Applicant(s)	
	10/814,608	LAIN ET AL.	
	Examiner	Art Unit	
	BRYAN WRIGHT	2431	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *18 December 2009*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-21* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-21* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This action is in response to amendment filed 12/18/2009. Claims 1-21 are pending.

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

2. Claims 13-20 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. Applicant's claims as recited are directed towards a method of consolidating key updates within a group environment. The Examiner contends applicant's method as recited must be tied to a machine to eliminate the possibility of such a key consolidation operation being performed by physical hand.

3. Claim 21 is rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. Applicant's claim as recited is directed towards a method of providing key updates to members within a group environment. The Examiner contends applicant's method as recited must be tied to a machine to eliminate the possibility of such a key update operation being performed by physical hand.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

This application currently names joint inventors. In considering patentability of the claims under 35 U.S.C. 103(a), the examiner presumes that the subject matter of the various claims was commonly owned at the time any inventions covered therein were made absent any evidence to the contrary. Applicant is advised of the obligation under 37 CFR 1.56 to point out the inventor and invention dates of each claim that was not commonly owned at the time a later invention was made in order for the examiner to consider the applicability of 35 U.S.C. 103(c) and potential 35 U.S.C. 102(e), (f) or (g) prior art under 35 U.S.C. 103(a).

4. Claims 1-4, and 12-16 are rejected under 35 U.S.C. 103(a) as being unpatentable over Challener et al (US Patent Publication No. 2002/0059286 and Challener hereinafter) in view of Caronni et al. (US Patent No. 6,049,878 and Caronni hereinafter).

5. As to clams 1 and 13, Challener teaches an apparatus for consolidating key updates provided in records that each comprise an encrypted key (e.g., user

key) corresponding to a node of a key hierarchy and encrypted (i.e., wrapped) using a key (e.g., platform key) which is a descendant of that node (i.e., ...teaches user key 103 is a migratable private 2048 RSA key wrapped by the platform key 102 and used as a root for all of a user's migratable keys [par. 21]), hierarchy-node information for both the encrypted and encrypting keys [fig. 1], the apparatus comprising a communications interface (e.g., bus) for receiving said records (912, fig. 9);

Challener does not expressly teach: and key-version information for at least the encrypted key; and a manager for maintaining, on the basis of the received records, a key tree with nodes corresponding to nodes in said hierarchy, the manager being arranged to store in association with each tree node, for each encrypting key used in respect of the encrypted key associated with the node, the most up-to- date version of the encrypted key and its version information with any earlier versions being discarded.

However at the time of applicant's original filing the feature of localizing key version information was well known and would have been an obvious modification of the teaching of Challener as disclosed by Caronni. Caronni discloses: key-version information for at least the encrypted key (to provide key-version information [col.. 9, lines 65-67; col. 10, lines 1-11]); and a manager for maintaining, on the basis of the received records (to provide a managing means for updating key data (e.g. record) [col. 10, lines 5-12]), a key tree (e.g., sub-tree)

with nodes corresponding to nodes in said hierarchy (to provide sub-tree corresponding to a hierarchy node [fig. 4]), the manager being arranged to store in association with each tree node (to provide storing capability of key data [col. 10, lines 1-10]), for each encrypting key used in respect of the encrypted key associated with the node, the most up-to-date version (e.g., version information) of the encrypted key and its version information with any earlier versions being discarded (to provide means to provide the most up-to-date key information (e.g., key version data) [col. 10, lines 1-12]).

Therefore, given Challener's key tree infrastructure, a person of ordinary skill in the art would have recognized the advantage of modifying Challener to provide a more robust re-keying means, with the well known feature of distributing and maintaining updated key information (e.g., key version) locally as disclosed by Caronni, thereby lowering the time it would normally take to re-key Challener's tree infrastructure.

6. As to claims 2 and 14, Challener teaches an apparatus where the manager is arranged to store each said most up-to-date version (e.g., new migratable signing key) of a said encrypted key by storing the record containing the latter with any previously-stored record that is thereby superseded being discarded. [par. 25]

7. As to claim 3, Challener teaches a apparatus where the manager is arranged to store in association with each tree node [par. 27],

Challener does not expressly teach: along with the most up-to-date version of the corresponding encrypted key stored for each encrypting key used in respect of that encrypted key, version information for the encrypting key used to encrypt said most up-to-date version of the encrypted key, this version information being included in the record providing said most up-to-date version of the encrypted key. However at the time of applicant's original filing the feature of localizing key version information was well known and would have been an obvious modification of the teaching of Challener as disclosed by Caronni. Caronni discloses: along with the most up-to-date version (e.g., updated device information) of the corresponding encrypted key stored for each encrypting key used in respect of that encrypted key ,version information (e.g., updated device information) for the encrypting key used to encrypt said most up-to-date version (e.g., updated device information) of the encrypted key, this version information being included in the record providing said most up-to-date version of the encrypted key (to provide means to provide the most up-to-date key information (e.g., key version data) [col. 10, lines 1-12]).

Therefore, given Challener's key tree infrastructure, a person of ordinary skill in the art would have recognized the advantage of modifying Challener to provide a more robust re-keying means, with the well known feature of distributing and

maintaining updated key information (e.g., key version) locally as disclosed by Caronni, thereby lowering the time it would normally take to re-key Challener's tree infrastructure.

8. As to clams 4 and 16, Challener teaches an apparatus where the manager is arranged to replace the version of the encrypted key stored in association with a tree node for a particular encrypting key (i.e., ...teaches updating the local key storage means [[par. 27),

Challener does not expressly teach: with any subsequently received later version of that key provided the latter has been encrypted with a version of the encrypting key that is the same or later than the version used for encrypting the existing stored encrypted key. However at the time of applicant's original filing the feature of re-encryption utilizing new key version information was well known and would have been an obvious modification of the teaching of Challener as disclosed by Caronni. Caronni discloses: with any subsequently received later version of that key provided the latter has been encrypted with a version of the encrypting key that is the same or later than the version used for encrypting the existing stored encrypted key.(to provide re-encrypting capability utilizing subsequent generated encrypting key data [col. 8, lines 1-20].

Therefore, given Challener's key storage means, a person of ordinary skill in the art would have recognized the advantage of modifying Challener with the well

known feature of re-encryption utilizing subsequent key versions as disclosed by Caronni, thereby enhancing Challener's encryption capability.

9. As to claims 8 and 20, Challener teaches an apparatus where the manager is arranged to maintain said tree only in respect of keys corresponding to the nodes of a predetermined sub-hierarchy of said hierarchy and keys for the path from the head of this sub-hierarchy that terminates at the root of the hierarchy [fig. 1].

10. As to clam 12, Challener teaches a system comprising: the apparatuses at each level of said hierarchical arrangement, other than said first level [fig. 1], each being arranged to maintain its said tree only in respect of keys corresponding to the nodes of a respective predetermined sub- hierarchy of said key hierarchy and keys for the path from the head of this sub- hierarchy that terminates at the root of the key hierarchy [fig. 5].

Challener does not expressly teach: multiple apparatuses and a key-hierarchy manager for managing said key hierarchy in dependence on the addition and/or removal of members to a group and for outputting key update records reflecting changes made to the key hierarchy; the apparatuses being configured in a multiple-level hierarchical arrangement comprising a first-level apparatus arranged to receive the records output by the key-hierarchy manager, and one or more lower levels of apparatuses each arranged to receive the key tree, or a

subset of it, produced by a said apparatus at the next level up, the apparatuses at the lowest level of the hierarchical arrangement each being arranged to provide its key tree, or a subset of it, to a respective sub-group of members of said group;

However at the time of applicant's original filing the feature of a key-hierarchy manager was well known and would have been an obvious modification of the teaching of Challener as disclosed by Caronni. Caronni discloses: multiple apparatuses and a key-hierarchy manager for managing said key hierarchy in dependence on the addition and/or removal of members to a group and for outputting key update records reflecting changes made to the key hierarchy (to provide the capability for group participant removal [col. 9, lines 10-25]);

the apparatuses being configured in a multiple-level hierarchical arrangement comprising a first-level apparatus arranged to receive the records output by the key-hierarchy manager (to provide the capability to receive key update information (e.g., records) in a hierarchical key structure [fig. 4), and one or more lower levels of apparatuses each arranged to receive the key tree, or a subset of it (to provide a sub-tree (e.g. subset) arrangement [co;. 8, lines 40-50]), produced by a said apparatus at the next level up, the apparatuses at the lowest level of the hierarchical arrangement each being arranged to provide its key tree, or a subset of it, to a respective sub-group of members of said group (to provide a sub-tree (e.g. subset) arrangement [fig. 4]);

Therefore, given Challener's root key hierarchy, a person of ordinary skill in the art would have recognized the advantage of modifying Challener with the well known feature of key management as disclosed by Caronni, thereby enhancing Challener's root key hierarchy.

11. As to clam 15, Challener teaches a method where in said sub-step the version information of the encrypting key used to encrypt said most up-to-date version of the encrypted key is stored with the latter [par. 27].

12. Claims 5-7, 9-11, 17- 19 and 21 are rejected under 35 U.S.C. 103(a) as being unpatentable over Challener in view of Caronni, as applied to claims 1 and 13 above, and further in view of McDaniel et al. (US Patent Publication No. 2003/0126464 and McDaniel hereinafter).

13. As to claims 5-7, and 17- 19, although the combination Challener in view of Caronni illustrates features of applicant's invention, the combination does not disclose:

An apparatus further comprising a working-set generator for processing the key tree to generate a subset of the tree enabling, at least within a target failure rate, all clients associated with the key hierarchy to recover the current root key of the latter (claims 5 and 17).

An apparatus where the working set generator comprises control means for receiving feedback on the current root-key recovery failure rate and for controlling the size of said subset to approach the actual failure rate to said target failure rate (claims 6 and 18).

An apparatus according where the working set generator further comprises means for determining the likelihood of a tree node being required to enable recovery the current root key, these means being based on at least one of the age of the node, or of an encrypted key associated with it, and an estimate of the number of possible clients that will need the node (claims 7 and 19).

However at the time of applicant's original filing the feature target failure analysis within a group key management environment was well known and would have been an obvious modification of the combined teachings of Challener and Caronni as disclosed by McDaniel. McDaniel discloses:

An apparatus further comprising a working-set generator for processing the key tree to generate a subset of the tree enabling, at least within a target failure rate, all clients associated with the key hierarchy to recover the current root key of the latter (to provide the capability for a new participant event (representing a newly admitted member) may require the initiation of session rekeying, such that the creation of new process monitoring timers (for failure detection and recovery) [par. 101]). (claims 5 and 15)

An apparatus where the working set generator comprises control means for receiving feedback on the current root-key recovery failure rate and for

controlling the size of said subset to approach the actual failure rate to said target failure rate (to provide a mechanism feedback mechanism (e.g., detection) for failure analysis [par. 142]). (claims 6 and 18)

An apparatus according where the working set generator further comprises means for determining the likelihood of a tree node being required to enable recovery the current root key, these means being based on at least one of the age of the node, or of an encrypted key associated with it, and an estimate of the number of possible clients that will 15 need the node (to provide failure detection to be supported through a timed heartbeat detection mechanism [par. 249]). (claims 7 and 19)

Therefore, given the key management capability of Challener in view of Caronni, a person of ordinary skill in the art would have recognized the advantage of modifying Challener in view Caronni to provide a more robust key management means, with the well known feature of target failure analysis as disclosed by McDaniel, thereby enhancing the reliability of the re-key operation of Challener in view of Caronni.

14. As to claims 9 and 21, although Challener discloses features of applicant's claimed invention, Challenger does not disclose:

A system comprising apparatus, and a key-hierarchy manager for managing said key hierarchy in dependence on the addition and/or removal of members to a group, the key-hierarchy manager being arranged to output said

records both to currently available members of said group and to said apparatus as notification of the changes made by the key-hierarchy manager to the key hierarchy, said apparatus being arranged to provide said key tree, or a subset of it,

However at the time of applicant's original filing these features were well known and would have been an obvious modification of the teaching of Challener as disclosed by Caronni. Caronni discloses:

A system comprising apparatus, and a key-hierarchy manager for managing said key hierarchy in dependence on the addition and/or removal (e.g. revoked) of members to a group (to provide the capability for group participant removal [par. 59]), the key-hierarchy manager being arranged to output said records both to currently available members of said group and to said apparatus as notification of the changes made by the key-hierarchy manager to the key hierarchy (to provide the capability to transmit to group participants current member association [par. 66]), said apparatus being arranged to provide said key tree, or a subset of it (to provide key recover capability such that a subset (e.g., sub-tree) is generated with consolidated key information [par. 68]).

Therefore, given Challener's key tree infrastructure, a person of ordinary skill in the art would have recognized the advantage of modifying Challener with the well known feature of key management as disclosed by Caronni thereby enhancing the key data distribution within Challener's key tree infrastructure.

The combination of Challener in view of Caronni does expressly teach: to members of said group who subsequently become available as a consolidated notification of the changes made by the key-hierarchy manager to the key hierarchy whereby to enable these members to recover the current root key of the key hierarchy at least within a target failure margin.

However at the time of applicant's original filing the feature target failure analysis within a group key management environment was well known and would have been an obvious modification of the combined teachings of Challener and Caronni as disclosed by McDaniel. McDaniel discloses:

to members of said group who subsequently become available as a consolidated notification of the changes made by the key-hierarchy manager to the key hierarchy whereby to enable these members to recover the current root key of the key hierarchy at least within a target failure margin (to provide the capability for a new participant event (representing a newly admitted member) may require the initiation of session rekeying, such that the creation of new process monitoring timers (for failure detection and recovery) [par. 101]).

Therefore, given the key management capability of Challener in view of Caronni, a person of ordinary skill in the art would have recognized the advantage of modifying Challener in view Caronni to provide a more robust key management means, with the well known feature of target failure analysis as disclosed by

McDaniel thereby enhancing the reliability of the re-key operation of Challener in view of Caronni.

15. As to claim 10, although Challener discloses features of applicant's claimed invention, Challenger does not disclose: A system comprising apparatus and a key-hierarchy manager for managing said key hierarchy in dependence on the addition and/or removal of members to a group, the key-hierarchy manager being arranged to output said records to said apparatus, said apparatus being arranged to provide said key tree, or a subset of it,

However at the time of applicant's original filing these features were well known and would have been an obvious modification of the teaching of Challener as disclosed by Caronni. Caronni discloses:

A system comprising apparatus and a key-hierarchy manager for managing said key hierarchy in dependence on the addition and/or removal (e.g., revoked) of members to a group (to provide the capability for group participant removal [par. 59]), the key-hierarchy manager being arranged to output said records (e.g., key update information) to said apparatus (to provide key manager data (e.g. record) transmission capability [par. 45]), said apparatus being arranged to provide said key tree, or a subset of it (to provide key recover capability such that a subset (e.g., sub-tree) is generated with consolidated key information [par. 68]),

Therefore, given Challener's key tree infrastructure, a person of ordinary skill in the art would have recognized the advantage of modifying Challener with the well known feature of key management as disclosed by Caronni thereby enhancing the key data distribution within Challener's key tree infrastructure.

The combination of Challener in view of Caronni does expressly teach: to members of said group who subsequently become available as a consolidated notification of the changes made by the key-hierarchy manager to the key hierarchy whereby to enable these members to recover the current root key of the key hierarchy at least within a target failure margin.

However at the time of applicant's original filing the feature target failure analysis within a group key management environment was well known and would have been an obvious modification of the combined teaching of Challener and Caronni as disclosed by McDaniel. McDaniel discloses:

to members of said group who subsequently become available as a consolidated notification of the changes made by the key-hierarchy manager to the key hierarchy whereby to enable these members to recover the current root key of the key hierarchy at least within a target failure margin (to provide the capability for a new participant event (representing a newly admitted member) may require the initiation of session rekeying, such that the creation of new process monitoring timers (for failure detection and recovery) [par. 101]).

Therefore, given the key management capability of Challener in view of Caronni, a person of ordinary skill in the art would have recognized the advantage of modifying Challener in view Caronni to provide a more robust key management means, with the well known feature of target failure analysis as disclosed by McDaniel thereby enhancing the reliability of the re-key operation of Challener in view of Caronni.

16. As to claim 11, although Challener discloses features of applicant's claimed invention, Challenger does not disclose:

A system where the key-hierarchy manager and said apparatus form part of an anonymous group content distribution arrangement; the key tree, or a subset of it, being sent to group members in association with content encrypted with a key that is one of: the key-hierarchy root key, and - a key encrypted using the key-hierarchy root key and provided in encrypted form 15 along with the encrypted content. (claim 11)

However at the time of applicant's original filing these features were well known and would have been an obvious modification of the teachings of Challener as disclosed by Caronni. Caronni discloses:

A system where the key-hierarchy manager and said apparatus form part of an anonymous group content distribution arrangement; the key tree, or a subset of it (to provide sub-tree (e.g., sub-set) generation capability [fig. 3]), being sent (e.g., transmission) to group members in association with content

encrypted with a key that is one of: the key-hierarchy root key (to provide transmission of updated key data to associated group participants [col. 10, lines 20-35]), and a key encrypted using the key-hierarchy root key and provided in encrypted form along with the encrypted content (to provide encrypted content and encrypted data [col. 10, lines 20-35]). (claim 11)

Therefore, given Challener's key tree infrastructure, a person of ordinary skill in the art would have recognized the advantage of modifying Challener with the well known feature of key management as disclosed by Caronni thereby enhancing the key data distribution within Challener's key tree infrastructure.

Response to Arguments

The Examiner contends Caronni teaches if a participant missed some version changes, he must ask any member of the group or the group manager to provide him with a log of key version change messages.

Contact Information

Any inquiry concerning this communication or earlier communications from the examiner should be directed to BRYAN WRIGHT whose telephone number is (571)270-3826. The examiner can normally be reached on 8:30 am - 5:30 pm Monday -Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, William Korzuch can be reached on (571) 272-7589. The

fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/BRYAN WRIGHT/
Examiner, Art Unit 2431

/William R. Korzuch/
Supervisory Patent Examiner, Art Unit 2431